REVUE FRANÇAISE D'AUTOMATIQUE, INFORMATIQUE, RECHERCHE OPÉRATIONNELLE. INFORMATIQUE THÉORIQUE

MAURICE MIGNOTTE

Sur la complexité de certains algorithmes où intervient la séparation des racines d'un polynôme

Revue française d'automatique, informatique, recherche opérationnelle. Informatique théorique, tome 10, n° R2 (1976), p. 51-55.

<http://www.numdam.org/item?id=ITA_1976__10_2_51_0>

R.A.I.R.O. Information Théorique
(vol. 10, n° 8, août 1976, p. 51 à 55).

SUR LA COMPLEXITÉ DE CERTAINS ALGORITHMES OU INTERVIENT LA SÉPARATION DES RACINES D'UN POLYNOME (*)

par MAURICE MIGNOTTE (1)

Communiqué par J. Berstel.

Abstract. — *The computing time of many algorithms on polynomials is bounded below by a function of the minimal distance between distinct roots. We give a lower bound for this distance in the case of polynomials with Gaussian integer coefficients.*

1. INTRODUCTION

Depuis quelques années, et pour répondre à la demande de divers utilisateurs d'ordinateurs, des systèmes de plus en plus élaborés de manipulation formelle ont vu le jour. Le problème fondamental est celui du calcul formel sur les polynômes. En particulier, G. E. Collins a été le responsable du projet SAC (Symbolic Algebraic Calculation). Comme ces calculs ont pour objet la résolution de problèmes concrets, le contrôle de la précision des résultats finals a évidemment revêtu une grande importance. Les recherches dans cette direction sont en particulier illustrées par le récent article de Collins et Horowitz [1] sur la séparation des racines d'un polynôme.

Soit sep (P) la distance minimale entre les racines distinctes d'un polynôme P. Il est souvent utile de connaître une borne inférieure de cette quantité. En particulier, la complexité des algorithmes connus pour isoler les racines d'un polynôme est minorée par une puissance du logarithme de $(\text{sep}\,(P))^{-1}$; *voir* à ce sujet, par exemple, les articles de Heindel [4] et Pinkert [8].

L'article de Collins et Horowitz [1] est consacré à l'étude de la minoration de sep (P) dans le cas des polynômes à coefficients dans l'anneau des entiers de Gauss et dont les racines sont simples. Ces auteurs démontrent trois minorations de sep (P), « with the hope of stimulating further research on the

(*) Reçu octobre 1975.

(1) Université Louis-Pasteur, Centre de Calcul, Strasbourg, France.

problem ». Ces trois résultats sont tous impliqués par des estimations plus anciennes de Mahler [6] (et aussi de Güting [3]). Nous indiquerons ici comment on peut améliorer les résultats de Mahler et étudierons le problème de savoir si ces inégalités sont les meilleures possibles.

2. UNE INÉGALITÉ FONDAMENTALE

Soit P un polynôme de degré $d \geqq 2$ à coefficients complexes et de racines α_i,

$$P(X) = a_d X^d + \ldots + a_0 = a_d \prod_{i=1}^{d} (X - \alpha_i). \tag{1}$$

La distance minimale entre les racines de P est la quantité

$$\operatorname{sep}(P) := \min_{\alpha_i \neq \alpha_j} |\alpha_i - \alpha_j|,$$

avec la convention $\operatorname{sep}(P) = \infty$ si P n'a pas deux racines distinctes. On note $\| P \| = \max |a_i|$, la hauteur de P, et on pose

$$\| P \|_p = \left(\sum_{i=0}^{d} |a_i|^p \right)^{1/p} \quad \text{pour} \quad p = 1 \quad \text{et} \quad p = 2,$$

(On a $\| P \|_2 \leqq \| P \|_1$) et

$$M(P) = |a_d| \Pi \{ |\alpha_i| ; |\alpha_i| > 1 \}.$$

On a la majoration suivante

LEMME 1 : *La quantité $M(P)$ vérifie l'inégalité*

$$M(P) \leqq \| P \|_2.$$

Cette inégalité a été oubliée et retrouvée plusieurs fois. Elle figure déjà dans un article de Landau [5]. Des démonstrations purement algébriques figurent en [2] et [7]. Il est bien connu que le module d'une racine d'un polynôme unitaire est essentiellement majoré par sa hauteur (on a alors $|\alpha_i| \leqq \| P \| + 1$); l'inégalité ci-dessus montre que le produit de *toutes* les racines de P extérieures au cercle unité est majoré par $\sqrt{d+1}\, \| P \|$, résultat beaucoup plus fort (et souvent utile!).

3. MINORATION DE sep (P)

Le meilleur résultat qui figure dans [1], et s'applique au cas où P est un polynôme sans racine multiple et à coefficients dans $\mathbf{Z}[i]$, est la minoration

$$\operatorname{sep}(P) \geqq \frac{1}{2} (e^{1/2}\, d^{3/2}\, \| P \|)^{-d}.$$

Sous les mêmes hypothèses Mahler ([6], corollaire du théorème 2) démontre le résultat plus fort

$$\operatorname{sep}(P) > \sqrt{3}\, d^{-(d+2)/2} \,||P||_1^{-(d-1)}. \tag{2}$$

La démonstration de (2) résulte de la proposition suivante :

LEMME 2. [6] : Si $D(P)$ *désigne le discriminant du polynôme* P *on a l'inégalité*

$$\operatorname{sep}(P) > \sqrt{3}\, d^{-(d+2)/2} \,|D(P)|^{1/2} M(P)^{-(d-1)}.$$

et de la majoration

$$M(P) \leqq ||P||_1. \tag{3}$$

En remplaçant (3) par le lemme 1, on obtient la minoration :

THÉORÈME 1 : *On a l'inégalité*

$$\operatorname{sep}(P) > \sqrt{3}\, d^{-(d+2)/2} \,|D(P)|^{1/2} ||P||_2^{-(d-1)}.$$

COROLLAIRE : *Un polynôme sans racine multiple et à coefficients appartenant à l'anneau des entiers d'un corps quadratique imaginaire vérifie*

$$\operatorname{sep}(P) > \sqrt{3}\, d^{-(d+2)/2} \,||P||_2^{-(d-1)}.$$

▶ En effet, les hypothèses impliquent $|D(P)| \geqq 1$. ◀

REMARQUE : Güting traite le cas général d'un polynôme à coefficients complexes (possédant éventuellement des racines multiples). Ces résultats reposent sur (3) et sont donc améliorés en utilisant le lemme 1. A titre d'exemple, on obtient ainsi la minoration

$$\operatorname{sep}(P) \geqq |D(P)|^{1/2} (d^{(d/2)-1} \binom{d}{2} ||P||_1^{d/2} ||P||_2^{(d/2)-1})^{-1}.$$

4. SUR UN PROBLÈME DE COLLINS ET HOROWITZ

Comme dans [1], nous posons

$$L(d, H) = \operatorname{Min}\{\operatorname{sep}(P);$$
$$P \in \mathbf{Z}[X] \text{ sans racine multiple, } \deg P = d, \, ||P||_1 \leqq H\}.$$

Il est à peu près trivial que l'on a

$$\frac{1}{H} \ll L(2, H) \ll \frac{1}{H}$$

[où, comme d'habitude, $f(H) \ll g(H)$ signifie qu'il existe une constante positive C telle que l'on ait $f(H) \leqq C\, g(H)$].

août 1976.

Il est démontré dans [2] que l'on a

$$\frac{1}{H^3} \ll L(3, H) \ll \frac{1}{H}.$$

Notre corollaire [ou (2)] fournit la minoration

$$L(3, H) \gg \frac{1}{H^2}.$$

Cette inégalité ne peut être améliorée : considérer l'exemple suivant, dû à J. M. Deshouillers,

$$P_n(X) = (q_n X - p_n)(X^2 - 2),$$

où p_n/q_n est la n-ième convergente du développement en fraction continue de $\sqrt{2}$ [on a en effet $\| P_n \|_1 \leqq 9q_n$ et $|(p_n/q_n) - \sqrt{2}| = \text{sep}(P) \leqq {q_n}^{-2}$]. Donc

$$H^{-2} \ll L(3, H) \ll H^{-2},$$

ce qui résout le problème de l'encadrement de $L(3, H)$ posé en [1].

5. UNE GÉNÉRATION DU PROBLÈME PRÉCÉDENT

Le paragraphe précédent incite à poser la définition suivante

$$L(d) = \limsup_{H \to \infty} \frac{-\text{Log}\, L(d, H)}{\text{Log}\, H}.$$

PROBLÈME : A-t-on $L(d) = d - 1$?

Le paragraphe précédent montre que cette égalité est vraie pour $d = 2$ et $d = 3$. Le corollaire du théorème 1 montre que l'on a toujours $L(d) \leqq d - 1$. De plus, il est clair que L est une fonction croissante (au sens large). Nous nous proposons de démontrer une minoration non triviale de $L(d)$. On note $[x]$ la partie entière de x.

THÉORÈME 2 : *La fonction $L(d)$ vérifie*

$$\left[\frac{d+1}{2}\right] \leqq L(d) \leqq d - 1.$$

D'après ce qui précède, seule la minoration est à démontrer et il suffit de la vérifier pour d impair, disons $d = 2\delta + 1$. Nous aurons pour cela besoin du résultat suivant.

LEMME 3 : *Soit* α *un nombre algébrique réel de degré* $> \delta$. *Alors, pour tout* $\varepsilon > 0$, *il existe une infinité de nombres algébriques* β *de degré* $\leqq \delta$ *tels que*

$$|\alpha - \beta| < H(\beta)^{-\delta - 1 + \varepsilon},$$

où H (b) *désigne la hauteur du polynôme minimal de* b.

▶ C'est le théorème 71 de [9], p. 45. ◀

Démonstration du théorème 2.

▶ Soit $d = 2\delta + 1$. Considérons un nombre réel α fixé de degré $\delta + 1$. A chaque nombre algébrique β de degré $\leqq \delta$ vérifiant les hypothèses du lemme 3 correspond un polynôme P, de degré d, admettant α et β comme racines et vérifiant $\| P \| \ll H(\beta)$. On a alors

$$\operatorname{sep}(P) \leqq |\alpha - \beta| < H(\beta)^{-\delta - 1 + \varepsilon} \ll \| P \|^{-\delta - 1 + \varepsilon} = \| P \|^{-((d+1)/2) + \varepsilon}.$$

Donc $L(d) \geqq ((d + 1)/2) - \varepsilon$. La conclusion en résulte, du fait que ε est quelconque. ◀

BIBLIOGRAPHIE

1. G. E. COLLINS and E. HOROWITZ. *The Minimum Root Separation of a Polynomial*, Math. Comp., 28, n° 126, 1974, p. 589-597.
2. V. GONÇALVES. *L'inégalité de W. Specht*, Rev. Fac. de Ciências de Lisboa, 1, 1950, p. 167-171.
3. R. GÜTING. *Polynomials With Multiple Zeroes*, Mathematika, 14, 1967, p. 181-196.
4. L. E. HEINDEL. *Integer Arithmetic Algorithms for Polynomial Real Zero Determination*, J. Assoc. Comp. Mach., 18, 1971, p. 533-548.
5. E. LANDAU. *Sur quelques théorèmes de M. Petrovié relatifs aux zéros des fonctions analytiques*, Bull. Soc. Math. France, 33, 1905, p. 251-261.
6. K. MAHLER. *An Inequality for the Discriminant of a Polynomial*, Michigan Math. J., 11, 1964, p. 257-262.
7. M. MIGNOTTE. *An Inequality About Factors of Polynomials*, Math. of Comp., 28, 1974, p. 1153-1157.
8. J. R. PINKERT. *Algebraic Algorithms for Computing the Complex Zeros of Gaussian Polynomials*, Ph. D. Thesis, Univ. of Wisconsin Comp. Sci. Dept., Technical Report n° 188, 1973.
9. W. M. SCHMIDT. *Approximation to Algebraic Numbers*, Monographie n° 19 de l'Enseignement Mathématique, Genève, 1972.

août 1976.